جامعة البعث
كلية العلوم
قسم الرياضيات

امتحان الفصل الأول 2018 – 2017
لمقرر : نظرية الأعداد

المدة :ساعة ونصف
الدرجة : 100

السؤال الأول(35 درجة) :

ليكن p عدداً أولياً ، و a,b عددين صحيحين، والمطلوب:

١) اثبت أنه إذا كان $p|ab$ فإن $p|a$ أو $p|b$.

٢) اثبت ان $\binom{p}{j} \mid p$ لكل $0 < j < p$.

٣) إذا كان $a^2 \equiv b^2 (\bmod p)$ فاثبت أن: $a \equiv b (\bmod p)$ أو $a \equiv -b (\bmod p)$.

السؤال الثاني (30 درجة) :

١) اكتب القاسم المشترك الأعظم للعددين: 20 ؛ 44، كتركيب خطي لهما.

٢) حل المعادلة: $44x + 20y = 600$ ، وأوجد حلولها الموجبة (في حال وجودها).

السؤال الثالث(35 درجة) :

ليكن m,n عددين صحيحين موجبين أوليين فيما بينهما، والمطلوب:

١) أثبت أن : $n^{\varphi(m)} \equiv 1 \pmod m$ ، حيث $\varphi(m)$ قيمة دالة أولر من أجل العدد m.

٢) أثبت ان: $\left[m^{\varphi(n)} + n^{\varphi(m)}\right] \equiv 1 \pmod{mn}$.

٣) أوجد مرتبة العدد 7 بالمقاس 20 ، وبين إن كان جذراً أولياً (أصلياً) للعدد 20.

د . ياسين خلوف

سلم تصحيح امتحان نظرية الأعداد - الفصل الأول 2017 - 2018 د. [illegible]

السؤال الأول (35)

1- إذا كان $p|a$ تم المطلوب، أما إذا كان $p\nmid a$ فإن $\gcd(p,a)=1$ ومنه يوجد $s,t\in\mathbb{Z}$ بحيث أن $ps+at=1$ وبالتالي $b(ps)+b(at)=b$

أي أن $(bs)\cdot p+(ab)t=b$ وبما أن $p|ab$ فرضاً و $p|(bs.p)$ فيجب

أن $p|[(bs)p+(ab)t]=b$ أي أن $p|b$.

إذن بالفعل إذا كان $p|ab$ فإن $p|a$ أو $p|b$

. وإذا لم يكن p عدداً أولياً فالقضية غير صحيحة بعض الأمثلة $6|12=3\cdot 4$ و $6\nmid 3$ و $6\nmid 4$

2- $$\binom{p}{j}=\frac{p(p-1)(p-2)\cdots(p-j+1)}{j!}=\frac{p!}{j!\,(p-j)!}$$

ومنه نكون

$$j!\binom{p}{j}=p(p-1)\cdots(p-j+1)$$

أن p تقسم الطرف الأيمن ومنه تقسم الأيسر أي $p\,|\,j!\cdot\binom{p}{j}$ ولكن

p عدد أولي فيجب أن يقسم $j!$ أو $\binom{p}{j}$:

فلو كان $p|j!$ أي أن $p|j(j-1)\cdots 3\cdot 2\cdot 1$ فيجب أن يقسم

أحد العوامل ولكن جميع العوامل أصغر تماماً من p حيث $0<j<p$

إذن p لا يمكن أن يقسم أياً منها ومنه p لا يقسم $j!$ وعليه

$p|\binom{p}{j}$. وهو المطلوب.

. إن شرط p أولي ضروري مثلاً: $4\nmid\binom{4}{2}=6$

3- إذا كان $a^2\equiv b^2 \pmod p$ فإن $p|(a^2-b^2)$ أي $p|(a-b)(a+b)$

ومنه $p|(a-b)$ أو $p|(a+b)$ أي أن $a\equiv b \pmod p$ أو $a\equiv -b \pmod p$

السؤال الثاني (30)

$$\left.\begin{array}{l}44=2\cdot 20+4\\ 20=5\cdot 4+0\end{array}\right\}\Rightarrow d(44,20)=4 \quad ,\quad 4=44-2(20)=44+(-2)(20)$$

إذن $4=1(44)+(-2)(20)$

ومنه

$$600=(150)(4)=(150)[(1)44+(-2)(20)]=44(150)+20(-300)$$

إذن $x_0=150$ و $y_0=-300$ والحل العام هو

$$\left.\begin{array}{l}x=150+\frac{20}{4}t\\ y=-300-\frac{44}{4}t\end{array}\right. ,\ t\in\mathbb{Z} \Rightarrow \left\{\begin{array}{l}x=150+5t\\ y=-300-11t\end{array}\right. ,\ t\in\mathbb{Z}$$

توجد الحلول موجبة عندما تتحقق المتراجحتان: $t \in \mathbb{Z}$ و

$$150+5t>0$$
$$-300+11t>0$$ أي

$$\left.\begin{array}{l}5t>-150\\ 11t<-300\end{array}\right\} \Rightarrow \left.\begin{array}{l} t>-30 \\ t<-\frac{300}{4}=-27,27\end{array}\right\} \Rightarrow t=-29, t=-28$$

عندئذ الحلول الموجبة للمعادلة هي:

$$t=-29: \quad x=150+5(-29)=\boxed{5},\quad y=-300-11(-29)=\boxed{19}$$ و or: $$t=-28: \quad x=150+5(-28)=\boxed{10},\quad y=-300-11(-28)=\boxed{8}$$

السؤال الثالث (35)

أ) إن رتبة $U(Z_m)$ تساوي $\varphi(m)$ أي أن $|U(Z_m)|=\varphi(m)$

حيث $\varphi(m)$ دالة أولر (قيمة أولر عند العدد m هي عدد الأعداد الطبيعية الأولية مع m والأصغر من n)

ومنه حسب مبرهنة لاغرانج ونتائجها نكون من أجل أي n أولي مع m:

$$\bar{n} \in U(Z_m) \Rightarrow (\bar{n})^{\varphi(m)} = \bar{1} \Rightarrow (n)^{\varphi(m)} = \bar{1} \Rightarrow$$

بالانتقال إلى الأعداد نكون

$$n^{\varphi(m)} \equiv 1 \pmod m$$

ب) حسب (أ) نكون

$$n^{\varphi(m)} \equiv 1 \pmod m \Leftrightarrow m \mid [n^{\varphi(m)}-1]$$
$$m^{\varphi(n)} \equiv 1 \pmod n \Leftrightarrow n \mid [m^{\varphi(n)}-1]$$

وبما أن $d(m,n)=1$ نكون

$$m \cdot n \mid (n^{\varphi(m)}-1)(m^{\varphi(n)}-1)$$ أي

$$m \cdot n \mid [m^{\varphi(n)} \cdot n^{\varphi(m)} - (m^{\varphi(n)} + n^{\varphi(m)}) + 1]$$

وحيث أن

$$m \mid m^{\varphi(m)} \text{ و } n \mid n^{\varphi(m)} \Rightarrow m \cdot n \mid m^{\varphi(n)} \cdot n^{\varphi(m)}$$

إذن بحسب (أ) نكون

$$m n \mid [1-(m^{\varphi(n)} + n^{\varphi(m)})]$$

أي

$$\boxed{m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{m \cdot n}}$$

ج) إن مرتبة العدد 7 بالقياس 20 تقسم $\varphi(20)$ أي تقسم 8: لدينا

$\varphi(20)=8$ ومنه تكون المرتبة بين قواسم 8:

$$(7)^2=49 \equiv 9 \pmod{20}, \quad (7)^4 \equiv 81 \pmod{20} \equiv 1 \pmod{20}$$

إذن $ord_{20}(7)=4 \neq \varphi(20)$ ولذلك 7 ليس جذراً أولياً